CLAIMS

What is claimed is:

1. A method of tracking incoming transmissions comprising:

identifying an incoming transmission including at least one identifiable portion;

computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the identified portion, the fingerprint being substantially unique to the identified portion;

storing the computed fingerprint to generate a set of stored fingerprints;

receiving a set of comparison fingerprints corresponding to known portions, the comparison fingerprints being predetermined; and

comparing the stored fingerprints to the comparison fingerprints to identify stored fingerprints matching comparison fingerprints and, if a match is found, identifying the previous incoming transmission corresponding to the matching stored fingerprint.

2. The method of claim 1 wherein storing further comprises selectively storing, if the incoming transmission does not correspond to the comparison fingerprints, at least one fingerprint corresponding to the identifiable portions of the incoming transmission.

3. The method of claim 1 wherein computing the fingerprint value includes determining a signature and comparing comprises signature matching.

4. The method of claim 1 further comprising receiving at least one successive set of comparison fingerprints, and iteratively comparing the successive sets of comparison fingerprints to the stored fingerprints, wherein if a match is found, identifying a distribution set of the incoming message corresponding to the matching stored fingerprint and transmitting an indication of the match to the distribution set.

5. The method of claim 1 wherein the comparison fingerprints are virus signatures computed from known undesirable transactions.

6. The method of claim 1 further comprising

storing an indication of the subsequent disposition of the incoming transmission;

receiving a subsequent set of comparison fingerprints, the subsequent set indicative of refinements to the known portions;

matching the subsequent set to the stored fingerprints;

determining, based on the matching of the subsequent set, if the subsequent set of comparison fingerprint is indicative of an undesirable portion in the incoming transmission; and

selectively performing, based on the determining, a remedial action in response to the subsequent disposition.

7. The method of claim 6 wherein the subsequent disposition includes transmitting the incoming transmission to a list of successive recipients; and the remedial action is sending a notification to the successive recipients indicative of the matching incoming transmission.

8. The method of claim 1 wherein the incoming transmission further comprises a series of potentially harmful network transmissions, each of the incoming transmission operable to include malicious code, wherein the subsequent disposition includes delivery to at least one successive recipient and remedial action includes determining the successive recipients from the stored successive disposition and notifying each of the successive recipients.

9. The method of claim 1 wherein the determined undesirable portion did not indicate undesirable transmissions based on the comparing of a previous set of comparison fingerprints.

10. The method of claim 1 further comprising demarcating the incoming transmission into segments, each segment operable to yield a fingerprint, wherein comparing further comprises comparing each value in the set of comparison fingerprints with at least one of the segments.

11. The method of claim 1 further comprising

identifying a segment type of each segment, the segment type corresponding to the content included in the segment; and

categorizing each of the segments according to a heuristic, the heuristic indicative of a likelihood of the categorized segment including an undesirable transmission.

12. The method of claim 11 further comprising:

identifying a risk assessment of each of the segment types; and

storing the segment according to the identified risk assessment, storing further including identifying a duration.

13. The method of claim 12 wherein storing the segments further comprises storing the content of the segment with the corresponding fingerprint.

14. The method of claim 1 wherein the undesirable portions are selected from the group consisting of viruses, worms and Trojan horses included as an attachment according to an established mail protocol.

15. A method of computer virus prevention comprising:

maintaining a first set of undesirable content definitions, the set of undesirable content definitions indicative of malicious transmissions;

comparing incoming transmissions to the first set of undesirable content definitions, the comparison result identifying malicious transmissions;

computing an artifact indicative of the incoming transmission, the artifact operable to identify the corresponding incoming transmission and distinguishable from artifacts corresponding to other incoming transmissions;

selectively storing, based on the comparison of the first set, if the incoming transmission does not correspond with the first set of undesirable content definitions, at least one artifact corresponding to the incoming transmission;

receiving an indication of a malicious segment;

merging the indication of the malicious segment with the first set of undesirable content definitions to generate a second set of undesirable content definitions;

comparing the second set of undesirable content definitions with the artifacts corresponding to the stored incoming transmissions; and

determining, based on the comparing of the second set of undesirable content definitions to the stored artifacts of previously processed transmissions, the incoming transmissions including malicious segments.

16. The method of claim 16 wherein the incoming transmission is not indicated as including a malicious segment by the first set of undesirable content definitions and matches a successive set of undesirable content definitions.

17. A data communications device for tracking incoming transmissions comprising:

a server having a scanner operable to identify an incoming transmission including at least one identifiable portion;

a segmenter operable to compute for each identifiable portion in the incoming transmission, a fingerprint indicative of the identified portion, the fingerprint being substantially unique to the identified portion;

a repository operable to store the computed fingerprints as a set of stored fingerprints, the repository, the server further operable to receive a set of comparison fingerprints corresponding to known portions, the comparison fingerprints being predetermined; and

a comparator operable to compare the stored fingerprints to the comparison fingerprints to identify stored fingerprints matching comparison fingerprints and, if a match is found, identifying the previously processed incoming transmission corresponding to the matching stored fingerprint.

18. The data communications device of claim 17 wherein the repository further includes stored fingerprints including at least one fingerprint corresponding to the identifiable portions of the incoming transmission.

19. The data communications device of claim 17 wherein the segmenter is further operable to compute the fingerprint value by determining a signature and the comparator is operable to compare fingerprints via signature matching.

20. The data communications device of claim 17 wherein the mail server is in communication with a virus detection determiner and is operable to receiving at least one successive set of comparison fingerprints from the virus detection determiner, and further operable to iteratively compare the received successive set of comparison fingerprints to the stored fingerprints, and responsively to a match, identify a distribution set of the incoming message corresponding to the matching stored fingerprint and transmitting an indication of the match to the distribution set.

21. The data communications device of claim 17 wherein the comparison fingerprints are virus signatures computed from known undesirable transactions.

22. The data communications device of claim 17 wherein the repository is operable to store an indication of the subsequent disposition of the incoming transmission, the mail server further operable to:

receive a subsequent set of comparison fingerprints, the subsequent set indicative of refinements to the known portions;

match the subsequent set to the stored fingerprints;

determine, based on the matching of the subsequent set, if the subsequent set of comparison fingerprint is indicative of an undesirable portion in the incoming transmission; and

selectively perform, based on the determining, a remedial action in response to the subsequent disposition.

23. The data communications device of claim 22 wherein the mail server is further operable to transmitting the incoming transmission to a list of successive recipients, and sending a notification to the successive recipients indicative of the matching incoming transmission.

24. The data communications device of claim 17 wherein the incoming transmission further comprises a series of potentially harmful network transmissions, each of the incoming transmission operable to include malicious code, wherein the disposition reference is operable to store an indication of delivery to at least one successive recipient.

25. The data communications device of claim 17 wherein the determined undesirable portion did not indicate undesirable transmissions based on the comparing of a previous set of comparison fingerprints.

26. The data communications device of claim 17 wherein the segmenter is operable to demarcate the incoming transmission into segments, each segment operable to yield a fingerprint, wherein the comparator is operable to compare each value in the set of comparison fingerprints with at least one of the segments.

27. The data communications device of claim 26 wherein the segmenter is operable to:

identify a segment type of each segment, the segment type corresponding to the content included in the segment; and

categorize each of the segments according to a heuristic, the heuristic indicative of a likelihood of the categorized segment including an undesirable transmission.

28. The data communications device of claim 27 wherein the segmenter is further operable to identify a risk assessment of each of the segment types, and the stored fingerprints are operable to storing the segment according to the identified risk assessment, storing further including identifying a duration.

29. The data communications device of claim 28 wherein the stored segments further comprises the data content of the segment with the corresponding fingerprint.

30. A computer program product having a computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for tracking incoming transmissions comprising:

computer program code for identifying an incoming transmission including at least one identifiable portion;

computer program code for computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the identified portion, the fingerprint being substantially unique to the identified portion;

computer program code for storing the computed fingerprint to generate a set of stored fingerprints;

computer program code for receiving a set of comparison fingerprints corresponding to known portions, the comparison fingerprints being predetermined; and

computer program code for comparing the stored fingerprints to the comparison fingerprints to identify stored fingerprints matching comparison fingerprints and, if a match is found, identifying the previously received incoming transmission corresponding to the matching stored fingerprint.

31. A computer data signal having program code for tracking incoming transmissions comprising:

program code for identifying an incoming transmission including at least one identifiable portion;

program code for computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the identified portion, the fingerprint being substantially unique to the identified portion;

program code for storing the computed fingerprint to generate a set of stored fingerprints;

program code for receiving a set of comparison fingerprints corresponding to known portions, the comparison fingerprints being predetermined; and

program code for comparing the stored fingerprints to the comparison fingerprints to identify stored fingerprints matching comparison fingerprints and, if a match is found,

identifying the previously received incoming transmission corresponding to the matching stored fingerprint.

32. A data communications device for tracking incoming transmissions comprising:

means for identifying an incoming transmission including at least one identifiable portion;

means for computing, for each identifiable portion in the incoming transmission, a fingerprint indicative of the identified portion, the fingerprint being substantially unique to the identified portion;

means for storing the computed fingerprint to generate a set of stored fingerprints;

means for receiving a set of comparison fingerprints corresponding to known portions, the comparison fingerprints being predetermined; and

means for comparing the stored fingerprints to the comparison fingerprints to identify stored fingerprints matching comparison fingerprints and, if a match is found, identifying the previously received incoming transmission corresponding to the matching stored fingerprint.